Corso di Qualità del Servizio e Sicurezza

a.a. 2014-2015

Docente: Ing. P. Fazio

Contatti:

email: pfazio@dimes.unical.it

tel.: 0984-494786

Orario di ricevimento: Lunedì ore 16.00 (41/C VI piano)

Libri consigliati:

- William B. Stallings: 'Cryptography and Network Security', Prentice Hall, 4/E, 2006.
- James F. Kurose, Keith W. Ross: 'Computer Networking: a Top-Down Approach Featuring the Internet', PearsonEducation, 4rd Ed., 2008.
- Wang Z.: 'Internet Qos: Architectures And Mechanisms For Quality Services', MORGAN KAUFMANN, 2001

Oltre il Best-Effort

L'Internet attuale

- L'Internet attuale fornisce un servizio best-effort a tutte le applicazioni.
- Non fa alcuna promessa sulla qualità del servizio (QoS) che un'applicazione riceve
- Un'applicazione riceverà qualsiasi livello di prestazioni che la rete è in grado di offrire in quel momento.
- L'Internet attuale non permette alle applicazioni multimediali (sensibili al ritardo) di richiedere alcun trattamento speciale.

L'Internet attuale

- Ai router i pacchetti sono trattati tutti allo stesso modo, compresi quelli sensibili al ritardo.
- Per rovinare la qualità di una chiamata IP in corso in Internet basta una quantità sufficiente di traffico che mandi la rete in congestione.
- Ciò causerà l'aumento dei ritardi e la perdita dei pacchetti.

L'Internet attuale

- Spesso in internet ogni connessione esiste solo per i due host alle sue estremità, che identificano tutti i pacchetti che si scambiano come appartenenti alla connessione stessa. Tali pacchetti, una volta usciti dall'host sorgente e prima di entrare in quello di destinazione, perdono la loro "reciproca parentela" e diventano entità indipendenti.
- Di conseguenza, le risorse della rete sono assorbite in modo del tutto incontrollato dai vari flussi di pacchetti e le prestazioni ottenute variano in modo quasi casuale a seconda del livello momentaneo di congestione.

Qualità del Servizio (QoS)

- Alcune connessioni sono involontariamente favorite dalla rete, mentre altre sono penalizzate; questo è il prezzo da pagare per avere una rete con architettura semplice e priva di tariffazione.
- I modelli di *QoS* per IP sono stati introdotti proprio per cambiare questa situazione e per dare la possibilità agli utenti (eventualmente paganti) di richiedere alla rete determinate prestazioni garantite.

QoS

- La *QoS* descrive il livello di prestazione che deve essere assicurato per una particolare applicazione.

- La *QoS* può essere definita in modo :
  - "*assoluto*" (***Performance Assurance***), definendo i valori che devono essere rispettati da un insieme di parametri "*prestazionali*" (es. ritardo massimo, probabilità di perdita di pacchetti, ecc),
  - o "*relativo*" (***Service Differentiation***), definendo le modalità di trattamento di una classe di traffico rispetto alle altre (es. livello di priorità di servizio, livello di priorità di scarto, ecc.).

QoS

- Una rete è in grado di garantire un fissato livello di *QoS* in due modi:
  - *Overprovisioning*: le risorse di rete sono dimensionate in modo che, nelle condizioni peggiori, il carico sia inferiore alla soglia minima di 'rottura', oltre la quale i contratti concordati con gli utenti non sono soddisfatti;
  - *Admission Control*: il traffico è controllato preventivamente e sarà accettato solo se le risorse di rete saranno sufficienti a garantire i livelli di qualità richiesti dagli utenti.

QoS

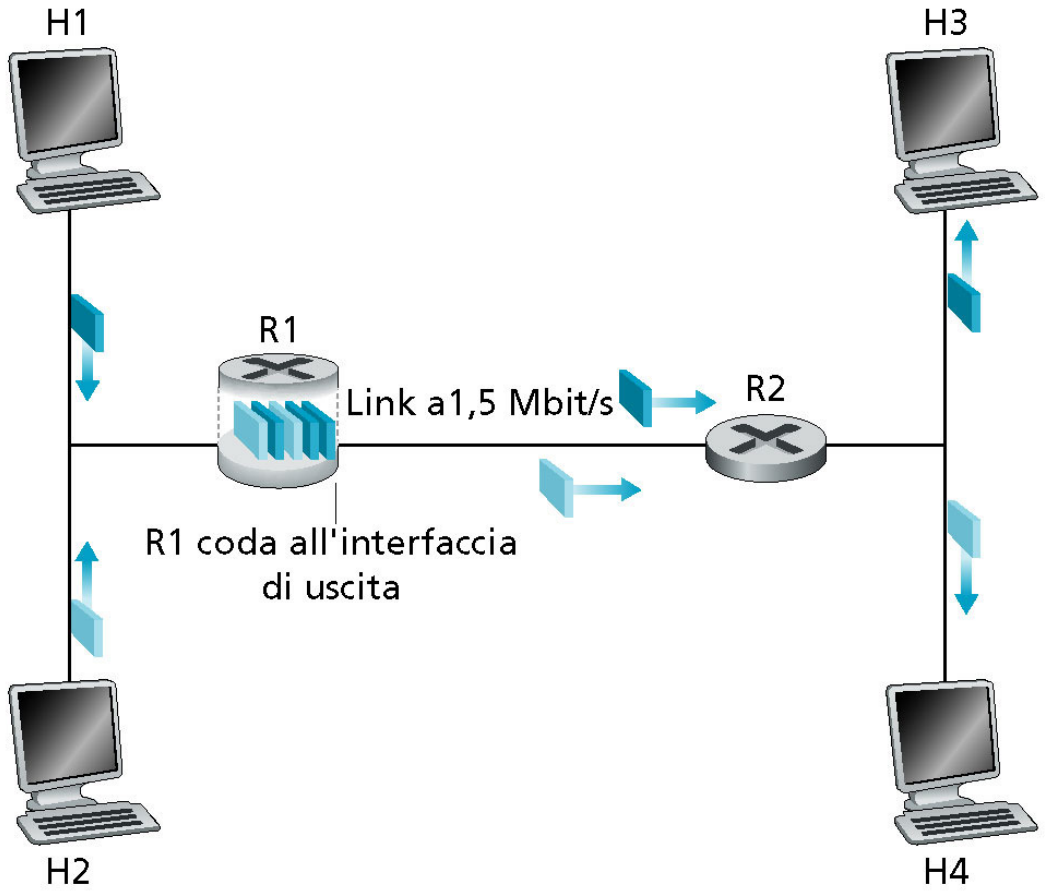
- La *QoS* può essere garantita:
- per *flusso*, per connessione, per chiamata
- per *aggregati* (o *classi*) di flussi, di connessioni, di chiamate.
- Un ***flusso*** è definito dalla 5-pla: *Source IP address*, *Source port number*, *Destination IP address*, *Destination port number*, *Protocol*.
- Una ***classe o aggregato di traffico*** comprende un insieme di flussi aventi requisiti simili di *QoS*.

QoS

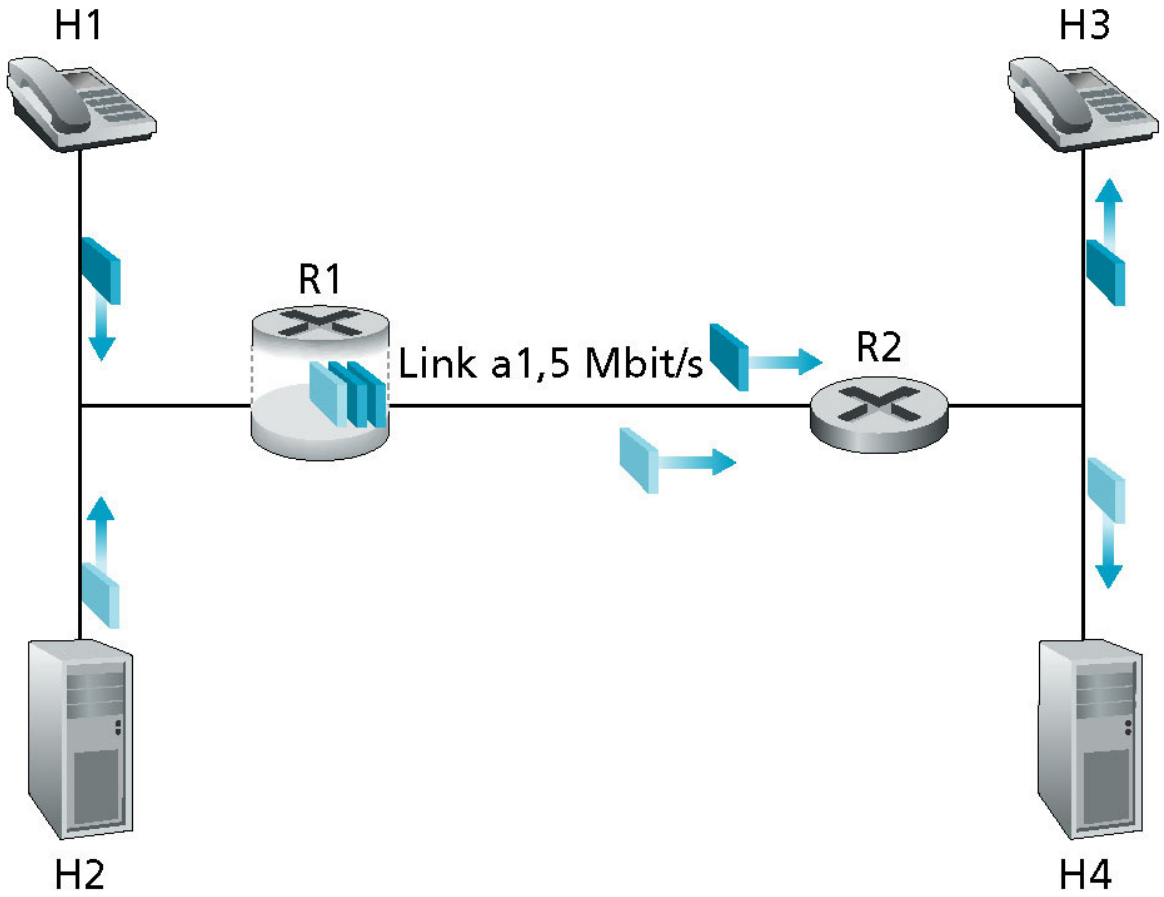
- Una politica di *QoS* orientata al trattamento dei singoli flussi (*per flow QoS*) assicura prestazioni migliori sia per quanto riguarda i singoli flussi che per quanto riguarda l'utilizzazione delle risorse di rete. Ha inoltre una notevole complessità dovuta ai meccanismi di segnalazione e alla necessità di monitorare i singoli flussi di pacchetti in rete nonché una bassa scalabilità.
- Una politica di *QoS* orientata al trattamento degli aggregati di flussi (*aggregate traffic QoS*) fornisce prestazioni non ottimali ma ha una complessità minore ed è maggiormente scalabile.

- Esistono diversi principi fondamentali della QoS, con i quali è possibile dotare l'architettura Internet di nuovi componenti strutturali, per proteggere un'applicazione da fenomeni come la congestione

Scenario di riferimento



Esempio 1: un'applicazione audio a 1 Mbs e un trasferimento FTP.



- Supponiamo di avere un'applicazione audio a 1 Mbs che condivide il link a 1,5 Mbs fra R1 e R2 con un'applicazione FTP che sta trasferendo file da H2 a H4.
- Nell'Internet best-effort i pacchetti audio e FTP sono mescolati nella coda in uscita da R1 e tipicamente trasmessi nell'ordine FIFO.
- Se una raffica di pacchetti FTP riempisse la coda causerebbe eccessivo ritardo o perdita di pacchetti audio per la saturazione della coda

- Come si può risolvere il problema?
- L'applicazione FTP non ha vincoli di tempo quindi potremmo dare una **priorità** ai pacchetti audio in R1
- Grazie alla priorità un pacchetto audio nel buffer di uscita di R1 dovrebbe essere trasmesso prima di qualsiasi pacchetto FTP
- Il link da R1 a R2 appare così come un link dedicato al traffico audio e FTP lo usa solo quando non c'è traffico audio accodato

I principio

- Perché R1 possa distinguere fra traffico audio e pacchetti FTP nella sua coda, ciascun pacchetto dovrà essere contrassegnato come appartenente a una delle due "classi" di traffico.

I principio

La **marcatura** dei pacchetti permette a un router di distinguere fra pacchetti appartenenti a due diverse classi di traffico.

- In realtà la marcatura esplicita è un mezzo con il quale distinguere i pacchetti. Il contrassegno portato da un pacchetto non può, di per sé, implicare che un pacchetto riceva una data QoS.
- La marcatura è un meccanismo per distinguere i pacchetti.
- Il modo in cui un router distingue tra i pacchetti per trattarli in modo diverso è una decisione politica

Esempio II: un'applicazione audio che si comporta in modo scorretto e un trasferimento FTP.

- Supponiamo ora che in qualche modo il router sappia che deve dare la priorità ai pacchetti dell'applicazione audio a 1 Mbs.
- Poiché la velocità del link in uscita è 1,5 Mbs anche se i pacchetti FTP ricevono una bassa priorità, essi riceveranno in media 0,5 Mbs.

- Ma cosa succede se l'applicazione audio comincia a inviare pacchetti al tasso di 1,5 Mbs o oltre?
- In questo caso **i pacchetti FTP non riceveranno alcun tipo di servizio** sul link R1-R2.
- Idealmente sarebbe desiderabile qualche grado di isolamento tra i flussi, per proteggere un flusso da un altro che si comporta in modo scorretto

II principio

II principio

E' desiderabile fornire un grado di isolamento tra i flussi di traffico, in modo che un flusso **non subisca gli effetti avversi** di un altro flusso che si comporta in modo scorretto

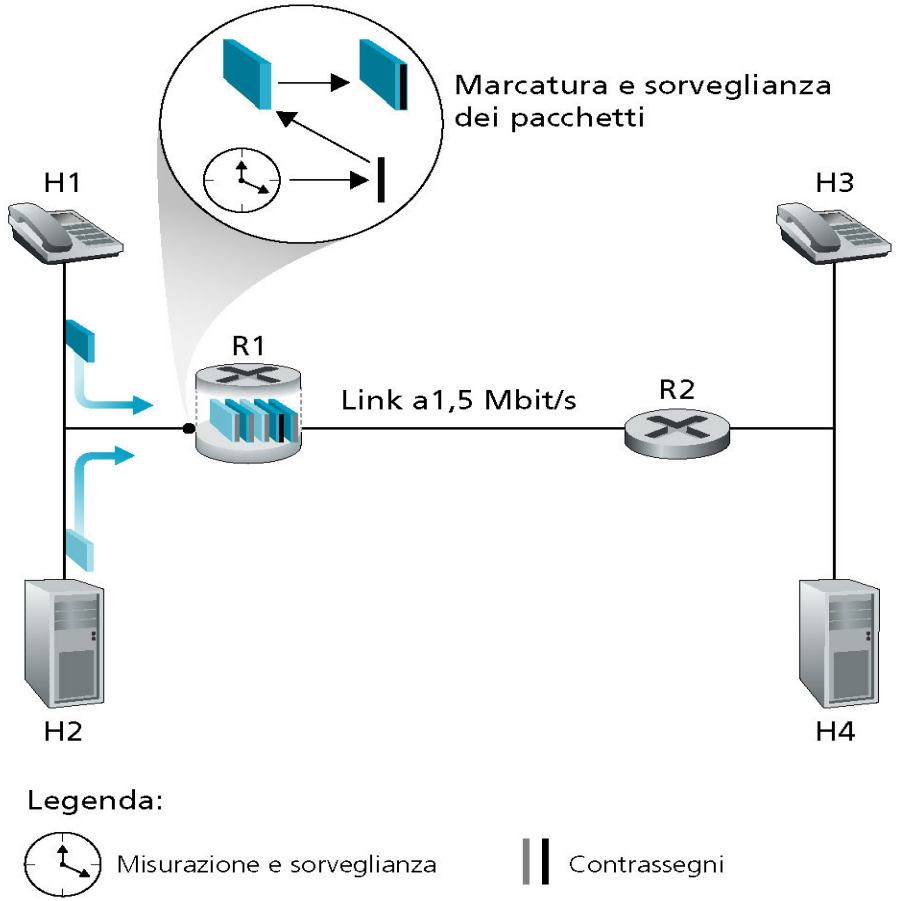
Si possono seguire due approcci:

- Sorvegliare i flussi di traffico
- Assegnare ai flussi dei canali logici separati

Sorvegliare i flussi di traffico

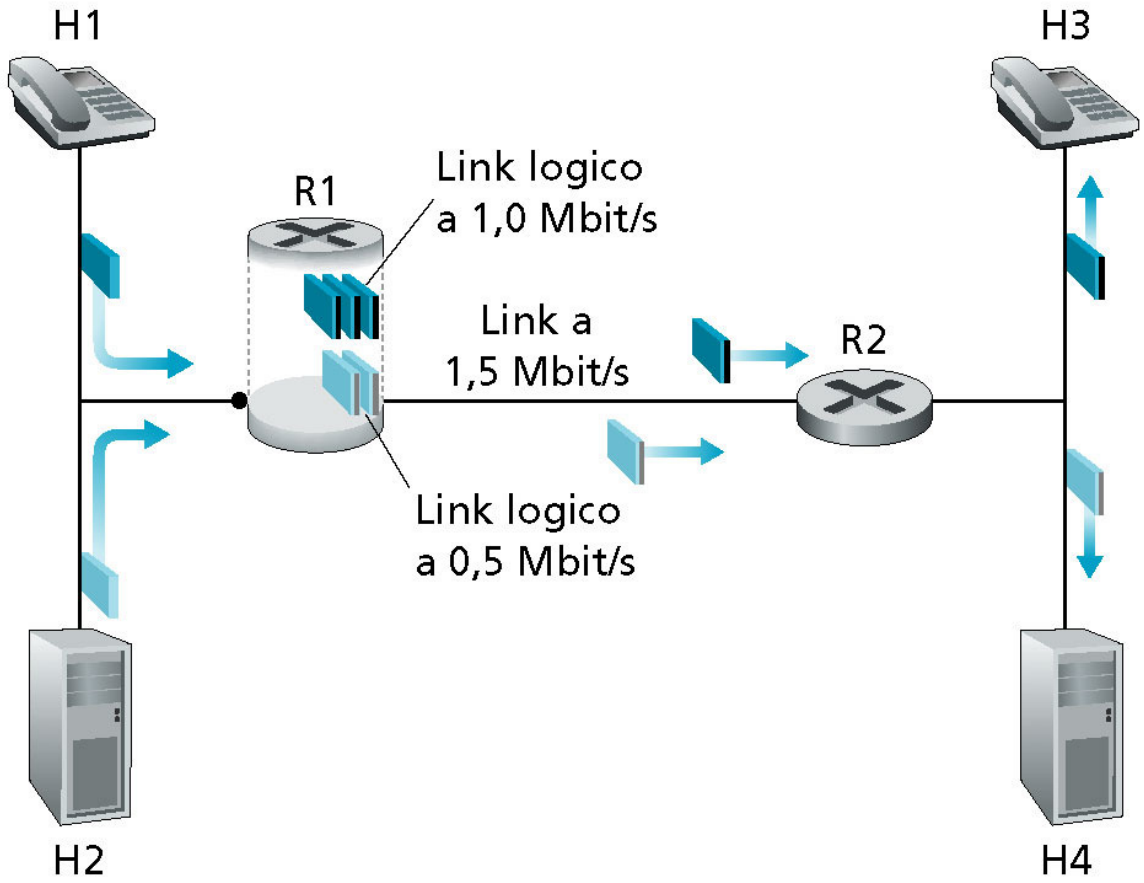
- Se un flusso di traffico deve soddisfare certi criteri (per es. il flusso audio non superi la velocità di picco di 1 Mbs) allora un meccanismo di sorveglianza può essere posto per assicurare che questo criterio sia rispettato.
- Se l'applicazione esaminata si comporta in modo scorretto, il meccanismo di sorveglianza prenderà alcune decisioni. (es. scartando o ritardando i pacchetti che violano i criteri)

- Il Token Bucket è il meccanismo di sorveglianza (policing) più usato



Assegnare ai flussi dei canali logici separati

- L'altro approccio per fornire l'isolamento tra i flussi prevede un meccanismo di scheduling dei pacchetti che a livello di link assegni esplicitamente a ciascun flusso una quantità fissa di larghezza di banda.
- Es. In R1 al traffico audio potrebbe essere assegnato 1 Mbs e al flusso FTP 0,5 Mbs. Così da vedere dei link logici con capacità di 1,0 e 0,5 Mbs.


H1
H3
R1
Link logico
a 1,0 Mbit/s
Link a
1,5 Mbit/s
R2
Link logico
a 0,5 Mbit/s
H2
H4

- Con un preciso controllo della larghezza di banda allocata a livello di link, un flusso può impiegare solo la larghezza di banda che gli è stata assegnata: in particolare non può utilizzare la banda che al momento non è usata da altre applicazioni.
- E' desiderabile però utilizzare la banda nel modo più efficiente possibile.

III principio

III principio

Mentre si fornisce l'isolamento tra i flussi, è desiderabile usare le risorse (es. buffer e larghezza di banda) il più efficientemente possibile.

Esempio III: due applicazione audio a 1 Mbs su un link sovraccarico a 1,5 Mbs.

- Supponiamo, ora, di avere due connessioni audio a 1 Mbs che trasmettono i loro pacchetti su un link di 1,5 Mbs
- La velocità combinata dei due flussi (2 Mbs) eccede la capacità del link.
- Anche con classificazione e marcatura (I principio), isolamento dei flussi (II principio) e condivisione della banda non usata (III principio), di cui non c'è traccia, chiaramente non si può fare molto.

- Non c'è abbastanza banda per soddisfare le necessità delle applicazioni
- Se esse si spartissero in modo uguale la capacità di banda del link riceverebbero 0,75 Mbs ciascuna.
- Le applicazioni perderebbero il 25% dei pacchetti trasmessi rendendole inutilizzabili a causa della bassa qualità ricevuta.

- Ad un flusso che richiede una minima qualità di servizio per essere considerato "utilizzabile", la rete dovrebbe garantire le condizioni per poter essere utilizzata oppure per impedirne l'utilizzo stesso.
- La rete telefonica è un esempio di rete che blocca le chiamate facendo risultare all'utente un segnale di occupato.
- Non c'è guadagno nel permettere a un flusso di accedere alla rete se non riceve la necessaria QoS da essere considerato "utilizzabile"
- Implicita con la necessità di fornire una QoS garantita a un flusso è la necessità che esso dichiari i suoi requisiti di QoS.

- Il processo di ammissione che fa sì che un flusso dichiari i suoi requisiti di QoS e che indichi alla rete di accettare il flusso oppure di bloccarlo è detto processo di **ammissione della chiamata**.

IV principio

E' necessario un processo di ammissione della chiamata in cui i flussi dichiarano i loro requisiti di QoS per poter essere ammessi alla rete (alla QoS richiesta) o bloccati dalla rete (se la QoS richiesta non può essere fornita)

Culture

Sommario dei principi